

A Generalization of Cover Free Families

Mehdi Azadi motlagh^{*} and Farokhlagha Moazami[†]

^{*}*Department of Mathematics*

Kharazmi University, 50 Taleghani Avenue, 15618, Tehran, Iran

`std_m.azadim@khu.ac.ir`

[†]*Cyberspace Research Center*

Shahid Beheshti University, G.C.

P.O. Box 1983963113, Tehran, Iran

`f_moazemi@sbu.ac.ir`

Abstract

An $(r, w; d)$ -cover-free family (CFF) is a family of subsets of a finite set such that the intersection of any r members of the family contains at least d elements that are not in the union of any other w members. The minimum number of elements for which there exists an $(r, w; d)$ -CFF with t blocks is denoted by $N((r, w; d), t)$. In this paper, we determine the exact value of $N((r, w; d), t)$ for some special parameters. Also, we present two constructions for $(2, 1; d)$ -CFF and $(2, 2; d)$ -CFF which improve the existing constructions. Moreover, we introduce a generalization of cover-free families which is motivated by an application of CFF in the key pre-distribution schemes. Also, we investigate some properties and bounds on the parameters of this generalization.

Key words: Biclique covering number, Cover-free families, Key pre-distribution.

Subject classification: 05B40.

1 Introduction

A *key pre-distribution scheme* (KPS) is a method by which a trusted authority (TA) distributes secret information among a set of users in such a way that every user in a group in some specified family of privileged subsets is able to compute a common key associated with that group. This common key must remain unknown to some specified coalitions of users (forbidden subsets) outside the privileged group. To construct a key pre-distribution scheme, TA can use a $\{0, 1\}$ -matrix M that is called *key distribution pattern*. A key distribution pattern specifies which users are to receive which keys. Namely, user u_i is given the key k_j if and only if $M[i, j] = 1$. Mitchell and Piper considered a key distribution pattern in which there is a key for every group of r users, such that this key is secure against any disjoint coalition of at most w users. A family of sets is called an (r, w) -cover-free family if no intersection of r sets of the family are covered by a union of any other w sets of the family. Easily one can see that Mitchell-Piper key distribution patterns are equivalent to (r, w) -cover-free families. Cover-free families were first introduced in 1964 by Kautz and Singleton in the context of superimposed binary codes [9]. Cover-free families (CFFs) were considered from different subjects such as combinatorics, information theory and group testing by many researchers (see, for example, [4, 5, 6, 7, 10, 14, 17, 18]). Stinson and Wei [17] have introduced a generalization of cover-free families as follows.

Definition 1. Let d, n, t, r , and w be positive integers and $B = \{B_1, \dots, B_t\}$ be a collection of subsets of a set X , where $|X| = n$. Each element of the collection B is called a block and the elements of X are called points. The pair (X, B) is called an $(r, w; d) - CFF(n, t)$ if for any two sets of indices $L, M \subseteq [t]$ such that $L \cap M = \emptyset$, $|L| = r$, and $|M| = w$, we have

$$|(\bigcap_{l \in L} B_l) \setminus (\bigcup_{m \in M} B_m)| \geq d.$$

Let $N((r, w; d), t)$ denote the minimum number of points of X in an $(r, w; d) - CFF$ having t blocks and $T((r, w; d), n)$ denote the maximum number of blocks in an $(r, w; d) - CFF$ with n points. ♠

An $(r, w; d)$ -cover-free family yields a key pre-distribution scheme in which every group of r users have at least d common keys that these keys are secure against any disjoint coalition of at most w users. The case $r = 2$ is of particular interest, because this is the case where keys are associated with pairs of users. Also, in the most applications, we do not need every 2-subset of users have a common key. In other word, for every key pre-distribution scheme that privileged subsets are 2-subsets, we can assign a graph as follows. Let the vertices of this graph be the users or nodes of the network and two vertices are adjacent if and only if these users or nodes can establish a common key. We name this graph the scheme graph. For instance, the scheme graph of key pre-distribution scheme constructed from a $(2, w; d)$ -cover free family is a complete graph. The definition of scheme graph leads us to the following generalization of cover-free families.

Definition 2. Let d, n, t , and w be positive integers and $B = \{B_1, \dots, B_t\}$ be a collection of subsets of a set X , where $|X| = n$. Assume that G is a graph with $V(G) = [t]$. The pair (X, B) , is called a $(G, w; d) - CFF(n, t)$ if for any two sets of indices $L, M \subseteq [t]$ such that $L \cap M = \emptyset$, $|L| = 2$, and L is an edge of G and $|M| = w$, we have

$$|(\bigcap_{l \in L} B_l) \setminus (\bigcup_{m \in M} B_m)| \geq d.$$

♠

This definition has a dual form as follows.

Definition 3. Let G be a graph and $\mathcal{A} = \{A_1, A_2, \dots, A_n\}$ be a collection of subsets of $V(G)$. The collection \mathcal{A} is called a (w, d) -covering of G if for every edge $\{u, v\}$ of the graph G and every w -subset, $W \subseteq V(G)$, disjoint from $\{u, v\}$, there exist at least d sets $A_{j_1}, \dots, A_{j_d} \in \mathcal{A}$ such that $\{u, v\} \subseteq A_{j_i}$ and $W \cap A_{j_i} = \emptyset$, for any $1 \leq i \leq d$. The number of sets in the minimum covering of G is called the *key pool number* of G and is denoted by $N(G, w; d)$. This parameter is denoted by $N(G)$ whenever $w = d = 1$. ♠

This generalization is a natural generalization for the set systems. For instance, Bollobás and Scott [2] consider a generalization like this for separating systems. In the following, we give a brief outline of graph theory which we need it. Throughout

this paper, we only consider finite simple graphs. For a graph G , let $V(G)$ and $E(G)$ denote its vertex and edge sets, respectively. In this paper, by $[n]$, we shall mean the set $\{1, 2, \dots, n\}$. The *biclique covering number* $bc(G)$ of a graph G is the smallest number of bicliques (complete bipartite subgraphs) of G such that every edge of G belongs to at least one of these bicliques. In the same manner, we can define *d-biclique covering number* $bc_d(G)$ of a graph G which is the smallest number of bicliques of G such that every edge of G belongs to at least d of these bicliques. In these cases, when the bicliques are required to be edge-disjoint, the corresponding measures are known as the *biclique partition number* and *d-biclique partition number* and are denoted by $bp(G)$ and $bp_d(G)$, respectively. Hajiabolhassan and Moazami [7] showed that the existence of an $(r, w; d)$ -cover-free family results from the existence of d -biclique cover of bi-intersection graph and vice versa. The *bi-intersection graph* $I_t(r, w)$ is a bipartite graph whose vertices are all w - and r -subsets of a t -element set, where a w -subset is adjacent to an r -subset if and only if their intersection is empty. They [6] also showed the existence of a secure frame proof code results from the existence of biclique cover of Kneser graph and vice versa. The *Kneser graph* $KG(t, r)$ is a graph whose vertices are all r -subsets of a t -element set, where two r -subsets are adjacent if and only if their intersection is empty. Motivated by these observations, we determine the exact value of d -biclique covering number of bi-intersection graph and Kneser graph for some special parameters in Section 2. For many applications of cover-free families, construction of cover-free families has been studied in the literature [13, 15, 16]. In Section 2, we also give a construction for $(2, 1; d)$ -cover-free family and a construction for $(2, 2; d)$ -cover-free family which improve the existing constructions. Moreover, in Section 3 we investigate some properties of (w, d) -covering of graphs and determine a relationship between this parameter and the biclique covering number of bipartite graphs.

2 Cover Free-Family

Determining the exact value of the parameter $N((r; w; d); t)$ and the biclique covering number of the Kneser graphs, even for special r , w , d , and t , is an interesting and challenging problem. This problem has been studied in the literature; see [6, 7, 11, 12, 13]. In this section, we determine the exact value of $N((r; w; d); t)$ for some special values of r , w , d , and t . Also, we determine the exact value of the biclique covering number of some Kneser graphs. To do this, we present a preliminary lemma as follows.

Lemma 1. *Let k and t be positive integers, where $2 \leq k \leq t$. Then*

$$B(KG(2t, k)) = B(I_{2t}(k, k)) = \binom{t}{k}^2,$$

where $B(G)$ is the maximum number of edges among the bicliques of G .

Proof. One can check that the maximum number of edges among the bicliques of each of these graphs is

$$\max_{k \leq i \leq t} \left[\binom{i}{k} \binom{2t-i}{k} \right].$$

Let $f(i) = \binom{i}{k} \binom{2t-i}{k}$, where $k \leq i \leq t$. Since $\frac{f(i-1)}{f(i)} = \frac{(i-k)(2t-i+1)}{i(2t-i-k+1)}$, it is easy to check that f is an increasing function. Hence,

$$B(KG(2t, k)) = B(I_{2t}(k, k)) = \binom{t}{k}^2,$$

as desired. ■

Theorem 1. *If $1 \leq k \leq t$ and $d = \binom{2t-2k}{t-k}$, then*

$$N((k, k; d), 2t) = bc_d(I_{2t}(k, k)) = bp_d(I_{2t}(k, k)) = \binom{2t}{t}.$$

Proof. Define t' to be $\binom{2t}{t}$. Now, we show that $I_{2t}(k, k)$ can be covered by t' bicliques such that every edge of $I_{2t}(k, k)$ is covered by exactly d bicliques. Denote the vertex set of $I_{2t}(k, k)$ by bipartition (X, Y) in which X and Y are the collections of all t -subsets of the set $[2t]$. Suppose A_j is a t -subset of $[2t]$ and A_j^c is the complement of the A_j in $[2t]$. Denote the number of these pairs by t' . Now, for every $1 \leq j \leq t'$, construct the biclique G_j with vertex set (X_j, Y_j) , where X_j is all k -subsets of A_j and Y_j is all k -subsets of A_j^c . Let UV be an arbitrary edge of $I_{2t}(k, k)$. In view of the definition of G_j , UV is covered by every G_j with vertex set (X_j, Y_j) , where U is a vertex of X_j and V is a vertex of Y_j or vice versa. Thus every edge of $I_{2t}(k, k)$ is covered by at least d bicliques. One can see that

$$\sum_{j=1}^{t'} |E(G_j)| = \binom{2t}{t} \binom{t}{k}^2 \quad \& \quad |E(I_{2t}(k, k))| = \binom{2t}{k} \binom{2t-k}{k}.$$

Now, it is simple to check that

$$\sum_{j=1}^{t'} |E(G_j)| = d |E(I_{2t}(k, k))|.$$

Thus every edge of $I_{2t}(k, k)$ is covered by exactly d bicliques. Note that we have actually proved that

$$bp_d(I_{2t}(k, k)) \leq t'. \tag{1}$$

Conversely, one can see that

$$bp_d(I_{2t}(k, k)) \geq bc_d(I_{2t}(k, k)) \geq \frac{d |E(I_{2t}(k, k))|}{B(I_{2t}(k, k))}.$$

Also, by Lemma 1, we have

$$\frac{d |E(I_{2t}(k, k))|}{B(I_{2t}(k, k))} = \frac{\binom{2t-2k}{t-k} \binom{2t}{k} \binom{2t-k}{k}}{\binom{t}{k}^2} = \binom{2t}{t} = t'.$$

Hence,

$$bp_d(I_{2t}(k, k)) \geq bc_d(I_{2t}(k, k)) \geq t'. \tag{2}$$

From (1) and (2) we conclude

$$bp_d(I_{2t}(k, k)) = bc_d(I_{2t}(k, k)) = t',$$

which completes the proof. ■

In view of the proof of the previous theorem, by a slight modification, one can obtain the following result.

Theorem 2. *If $1 \leq k \leq t$ and $d = \binom{2t-2k}{t-k}$, then*

$$bc_d(KG(2t, k)) = bp_d(KG(2t, k)) = \frac{\binom{2t}{t}}{2}.$$

There are many applications for cover-free families. Consequently, the efficient construction of cover-free families is an interesting problem for researchers. Li et al. [13] proved the following theorem.

Theorem A. [13] *If there exists a $(2, 1; d) - CFF(n, t)$, then there exists a $(2, 1; d) - CFF(n + (s + 2)(d + 1), 2t)$, where $s = N((1, 1), t)$.*

In the next theorem, we give a construction which improves Theorem A.

Theorem 3. *If there exists a $(2, 1; d) - CFF(n_1, t)$ and a $(1, 1; d) - CFF(n_2, t)$, then there exists a $(2, 1; d) - CFF(n_1 + n_2 + 2, 2t)$.*

Proof. Let $\mathcal{P} = \{G_1, \dots, G_{n_1}\}$ and $\mathcal{A} = \{K_1, \dots, K_{n_2}\}$ be a d -biclique cover of $I_t(1, 2)$ and $I_t(1, 1)$, respectively. Also, assume that G_i and K_i have (X_i, Y_i) and (W_i, Z_i) as vertex sets, respectively. For $i = 1, \dots, n_1$, let E_i be the union of all 2-subsets of Y_i . Suppose that $\{1, 2, \dots, t, 1', 2', \dots, t'\}$ is the ground set of the vertex set of the graph $I_{2t}(1, 2)$. In the sequel, for any $A \subseteq [t]$, A' stands for the set $\{i' | i \in A\}$. Let A_i and C_i be the set of all 1-subsets of the set $X_i \cup X'_i$ and $Z_i \cup Z'_i$, respectively. Also, let B_i and D_i be the set of all 2-subsets of the set $E_i \cup E'_i$ and $W_i \cup W'_i$, respectively. Let H_i and L_i be two bicliques in which (A_i, B_i) and (C_i, D_i) are the bipartition of their vertex sets, respectively. Also, let H be a biclique that has (A, B) as the bipartition of its vertex set, where A contains all 1-subsets of the set $[t]$ and B contains all 2-subsets of the set $\{1', \dots, t'\}$. Similarly, let K be a biclique with (Z, W) as the bipartition of its vertex set, where Z contains all 1-subsets of the set $\{1', \dots, t'\}$ and W contains all 2-subsets of the set $[t]$. Easily one can check that the set $\{H_1, \dots, H_{n_1}, L_1, \dots, L_{n_2}, H, K\}$ form a d -biclique cover for the graph $I_{2t}(1, 2)$. ■

The proof of the next theorem is analogous to that of Theorem 3.

Theorem 4. *If there exists a $(2, 2; d) - CFF(n_1, t)$ and a $(2, 1; d) - CFF(n_2, t)$, then there exists a $(2, 2; d) - CFF(n_1 + 2n_2 + 2, 2t)$.*

3 Generalization of Cover-Free Families

Assume that G is a graph with t vertices and $\delta(G) > w$. Let $\mathcal{A} = \{A_1, A_2, \dots, A_n\}$ be an optimal covering of G . Assume that v is an arbitrary vertex of the graph G and W is a w -subset of vertices such that $v \notin W$. Since $\delta(G) > w$, there exists a vertex u adjacent to v such that $u \notin W$. In view of the definition of a covering, there exists $\{i_1, \dots, i_d\}$ such that, for each $k = 1, 2, \dots, d$, $\{u, v\} \subseteq A_{i_k}$ and $W \cap A_{i_k} = \emptyset$. So we have $N((1, w; d), t) \leq N(G, w; d)$.

Lemma 2. *If G is a graph with m edges, then*

$$m \leq T((1, w; d), N(G, w; d)).$$

Proof. Let $\mathcal{A} = \{A_1, A_2, \dots, A_n\}$ be an optimal (w, d) -covering of G , i.e., $n = N(G, w; d)$. Set

$$\mathcal{B} = \{K_i \cap K_j \mid ij \in E(G)\},$$

where K_i is the set of keys of the i^{th} user. It is easy to see that \mathcal{B} is a $(1, w; d)$ -CFF with m blocks and n elements. Hence, $m \leq T((1, w; d), n)$. \blacksquare

An antichain $\{A_1, A_2, \dots, A_t\}$ on a set A is a family of nonempty subsets of A such that $A_i \subseteq A_j$ implies that $i = j$. In fact, an antichain with t block on the set $[n]$ is a $(1, 1) - \text{CFF}(n, t)$. By Sperner's lemma, if $\mathcal{A} = \{A_1, A_2, \dots, A_t\}$ is an antichain on the set $[n]$, then $t \leq \binom{n}{\lfloor \frac{n}{2} \rfloor}$. Hence, $T((1, 1); n) \leq \binom{n}{\lfloor \frac{n}{2} \rfloor}$ and if $\mathcal{R}(t) = \min\{c \mid \binom{c}{\lfloor \frac{c}{2} \rfloor} \geq t\}$, then $\mathcal{R}(t) = N((1, 1), t)$. Note that, by Sterling's formula, $\mathcal{R}(t) = \log_2 t + \frac{1}{2} \log_2 \log_2 t + O(1)$. Erdős et al. [4] discussed $(2, 1)$ -CFFs in detail, and showed that

$$1.134^n \leq T((2, 1), n) \leq 1.25^n.$$

The upper bound is asymptotic and for sufficiently large n is useful. Here is the best known lower bound for $N((1, w), t)$.

Theorem B. [3, 5, 14] *Let $w \geq 2$ and $t \geq w + 1$ be positive integers. Then*

$$N((1, w), t) \geq C_{w,t} \frac{w^2}{\log w} \log t,$$

where $\lim_{w+t \rightarrow \infty} C_{w,t} = c$ for some constant c .

In [3, 5, 14], it was shown that c is approximately $\frac{1}{2}$, $\frac{1}{4}$, and $\frac{1}{8}$, respectively. As a result of this lower bound, we have

$$T((1, w), n) \leq w^{\frac{n}{cw^2}}.$$

So the following corollary is concluded.

Corollary 1. *If G is a graph with m edges, then*

1. $\frac{2}{1+\log_2 e} \log_2 m \leq N(G),$
2. $\frac{1}{\log 1.25} \log m \leq N(G, 2; 1),$
3. $c \frac{w^2}{\log w} \log m \leq N(G, w; 1),$ for every $w \geq 2$.

Let K_{t_1, t_2} be the complete bipartite graph. In the next proposition, we give an upper bound for the $(1, d)$ -covering of these graphs.

Proposition 1. *If t_1, t_2 , and d are positive integers, then*

$$N(K_{t_1, t_2}, 1; d) \leq N((1, 1; d), t_1) + N((1, 1; d), t_2).$$

Proof. Label the vertices of the first and second part of K_{t_1, t_2} with v_1, v_2, \dots, v_{t_1} and u_1, u_2, \dots, u_{t_2} , respectively. Assume that $\{A_1, A_2, \dots, A_{n_1}\}$ and $\{S_1, S_2, \dots, S_{n_2}\}$ are optimal $(1, d)$ -covering of the complete graph with t_1 vertices and t_2 vertices respectively, i.e., $n_1 = N((1, 1; d), t_1)$ and $n_2 = N((1, 1; d), t_2)$. Define $A'_i = A_i \cup \{u_1, u_2, \dots, u_{t_1}\}$ for $i = 1, 2, \dots, n_1$ and $S'_i = S_i \cup \{v_1, v_2, \dots, v_{t_2}\}$ for $i = 1, 2, \dots, n_2$. One can check that the collection $\{A'_1, \dots, A'_{n_1}, S'_1, \dots, S'_{n_2}\}$ is a covering of the graph K_{t_1, t_2} and so

$$N(K_{t_1, t_2}, 1; d) \leq N((1, 1; d), t_1) + N((1, 1; d), t_2),$$

as desired. ■

By the lower bound of Corollary 1 and the upper bound of Proposition 1, for every positive integer t , we have

$$(1.637) \log_2 t \leq N(K_{t, t}) \leq 2N((1, 1), t) = 2\mathcal{R}(t) = 2 \log_2 t + \log_2 \log_2 t + O(1).$$

If for a graph G , there exists a covering of the edges of the complete graph K_t with l copies of G , then one can see that there exists a $(2, w; d) - CFF(lN(G, w; d), t)$. In [8], Katona and Szemerédi showed that the edges of the complete graph K_t can be covered by the complete bipartite graph $K_{\frac{t}{2}, \frac{t}{2}}$ with a collection of size $\log_2 t$. So we have the following corollary.

Corollary 2. *There exists a $(2, 1) - CFF(2\mathcal{R}(\frac{t}{2}) \log_2 t, t)$.*

In the next proposition, we show the relationship between $N(G)$ and biclique covering number of a special families of bipartite graphs.

Proposition 2. *Let G be a graph. There exists a bipartite graph H such that*

$$N(G, w; d) = bc_d(H).$$

Proof. Let H be a bipartite graph whose vertices are all edges and all w -subsets of vertices of the graph G . We say an edge, $e = \{u, v\}$, is incident to a w -subset W if and only if $W \cap \{u, v\} = \emptyset$. We claim that $N(G, w; d) = bc_d(H)$. To see this, first assume that the collection $\{G_1, \dots, G_l\}$ is a d -biclique cover of the graph H , where $l = bc_d(H)$ and G_i has (X_i, Y_i) as its vertex set. Let A_i be the union of the vertices of edges lying in X_i and B_i be the union of the vertices of w -subsets lying in X_i . Set $\mathcal{A} = \{A_1, A_2, \dots, A_l\}$. It is easy to check that \mathcal{A} is a (w, d) -covering of the graph G . So $N(G, w; d) \leq bc_d(H)$. Conversely, assume that $\mathcal{A} = \{A_1, A_2, \dots, A_l\}$ is an optimal (w, d) -covering of the graph G , i.e., $l = N(G, w; d)$. Now, for any $1 \leq j \leq l$, construct a bipartite graph G_j with the vertex set (X_j, Y_j) , where the vertices of X_j are all edges of G that its end points are elements of A_j and the vertices of Y_j are all w -subsets of the set A_j^c . Also, an edge is incident to a w -subset if their intersection is empty. So G_j is a complete bipartite subgraph of H . Let UV be an arbitrary edge of the graph H . Hence, there exists an edge $e = \{u, v\}$ of the graph G and a w -subset W of vertices disjoint from $\{u, v\}$ such that $U = \{u, v\}$ and $V = W$. Since \mathcal{A} is a (w, d) -covering of the graph G , there exist d indices i_1, \dots, i_d such that $e = \{u, v\} \subseteq A_{i_j}$, and $W \cap A_{i_j} = \emptyset$, for $j = 1, \dots, d$. Therefore, G_{i_1}, \dots, G_{i_d} covers UV and $\{G_1, G_2, \dots, G_l\}$ is a d -biclique cover of H . So $bc_d(H) \leq N(G, w; d)$. ■

Let $K_{t,t}^-$ be the graph $K_{t,t}$ with a perfect matching removed. Determining the biclique covering number of the $K_{t,t}^-$ was discussed by Bezrukov et al. [1]. Let G be a graph and S be a subset of the edges of G . The graph $G \setminus S$ is obtained from G by removing S . By the proof of Theorem 2, for every graph G with t vertices and m edges, we have

$$N(G) = bc(K_{m,t} \setminus K),$$

where K is a bipartite graph in which every vertex in the first part has degree 2 and every vertex in the second part has the same degree as the graph G . So we have the following corollary.

Corollary 3. *For every integer n , $N(C_n) = bc(K_{n,n} \setminus C_{2n})$.*

Lemma 3. *Assume that G_1, G_2, \dots, G_k are graphs such that for any $i = 2, \dots, k$, the graph G_1 contains a subgraph isomorphic to G_i . Then*

$$N(\cup_{i=1}^k G_i) \leq N(G_1) + k.$$

Proof. Let $\mathcal{A} = \{A_1, \dots, A_n\}$ be an optimal covering of the graph G_1 . For any $j \in \{2, \dots, k\}$, assume that $f_j : V(G_j) \rightarrow V(G_1)$ is an injective homomorphism, i.e., a one-to-one map which preserves the adjacency. For every $1 \leq i \leq n$, set $B_i = \{v \in V(G_j) \mid j = 2, \dots, k, f_j(v) \in A_i\}$ and $C_i = A_i \cup B_i$. One can check that the collection $\mathcal{C} = \{C_1, \dots, C_n, V(G_1), \dots, V(G_k)\}$ is a covering for the graph $\cup_{i=1}^k G_i$. ■

Lemma 4. *If G is a star graph with $t + 1$ vertices, then*

$$N(G, w; d) = N((1, w; d), t).$$

Proof. Let G be a star which v is the interval vertex and v_1, v_2, \dots, v_t are its leaves. Let $\mathcal{A} = \{A_1, A_2, \dots, A_n\}$ be a minimum (w, d) -covering of G . Since \mathcal{A} is a minimum covering, every A_i contains the vertex v . Consider the collection $\mathcal{S} = \{S_i \mid S_i = A_i \setminus \{v\}, i = 1, \dots, n\}$. One can see that the collection \mathcal{S} is a (w, d) -covering of a complete graph with t vertices. So, $N((1, w; d), t) \leq N(G, w; d)$. Conversely, consider an optimal $(1, w; d) - CFF(n, t)$ i.e., $n = N((1, w; d), t)$. Set $\mathcal{S} = \{S_1, S_2, \dots, S_n\}$, where S_i is the set of users that have i^{th} key. One can check that the collection $\{A_i \mid A_i = S_i \cup \{v\}, i = 1, \dots, n\}$ is a (w, d) -covering of G . Therefore, $N(G, w; d) \leq N((1, w; d), t)$. ■

Theorem 5. *Let T be a tree with m edges and maximum degree Δ . Also, assume that t is the number of vertices of T whose degrees are at least 3. Then*

$$N(T) \leq 2\lceil \log_2 m \rceil + \mathcal{R}(\Delta) + t.$$

Proof. We prove the theorem in two steps. First suppose that T is a path of length n . Assume that k is the smallest positive integer such that $2^k \geq n$. It is sufficient to prove the proposition for the path $P = P_{2^k+1}$. We decompose P into two edge-disjoint paths $P_{1,1}, P_{1,2}$ with the same length. Inductively, for each i such that $1 \leq i \leq k - 1, 1 \leq j \leq 2^i$, we decompose the path $P_{i,j}$ into two edge-disjoint

paths $P_{i+1,2j-1}, P_{i+1,2j}$ with the same length. Set $A_1 = V(P_{1,1})$ and $B_1 = V(P_{1,2})$. Also, for each i such that $2 \leq i \leq k-1$, define

$$A_i = \bigcup_{t=1}^{2^{i-2}} V(P_{i,4t}) \bigcup_{t=1}^{2^{i-2}} V(P_{i,4t-3}) \quad \& \quad B_i = \bigcup_{t=1}^{2^{i-2}} V(P_{i,4t-2}) \bigcup_{t=1}^{2^{i-2}} V(P_{i,4t-1}),$$

where $V(P_{i,j})$ is the vertex set of $P_{i,j}$. Now, we show that

$$\mathcal{A} = \{A_1, \dots, A_k, B_1, \dots, B_k\}$$

is a covering of the path P . Assume that uv is an arbitrary edge of P and w is a vertex of P other than u and v . In view of the definition of $P_{i,j}$'s, there exists a positive integer t such that $uv \in E(P_{t,j})$ and $w \notin V(P_{t,j})$. One can check that either $uv \in A_t$ and $w \notin A_t$ or $uv \in B_t$ and $w \notin B_t$, as desired. Let us now assume that T is a union of l paths where $l \geq 1$ and $\mathcal{V}' = \{v_1, v_2, \dots, v_t\}$ is the collection of vertices of T whose degrees are at least 3. Let $T' = T \setminus \mathcal{V}'$. One can check that T' is a union of vertex-disjoint paths with at most $m - 3t$ vertices. According to the first step of the proof, T' has a covering of size $2\lceil \log_2(m - 3t) \rceil$. Let S_i be the subgraph induced by the edges of T incident to v_i , for every i where $1 \leq i \leq t$. Since S_i , for every $1 \leq i \leq t$, is an star, by Lemmas 3 and 4, the subgraph induced by $\bigcup_{1 \leq i \leq t} S_i$ can be covered by a collection of size at most $\mathcal{R}(\Delta) + t$. This completes the proof of theorem. \blacksquare

By writing out a proof similar to that of Theorem 5 and by Corollary 3, we obtain the following result.

Corollary 4. *If C_n is a cycle of length n , then*

$$\mathcal{R}(n) \leq bc(K_{n,n} \setminus C_{2n}) = N(C_n) \leq 2\lceil \log_2 n \rceil + 1.$$

The *Cartesian product* of two graphs G and H denoted by $G \square H$ is a graph such that the vertices of $G \square H$ is the set $V(G) \times V(H)$ and two vertices (u, u') and (v, v') are adjacent if and only if either $u = v$ and u' is adjacent to v' in the graph H or $u' = v'$ and u is adjacent with v in the graph G .

Corollary 5. *If t_1 and t_2 are positive integers, then*

$$N(P_{t_1} \square P_{t_2}) \leq 2\lceil \log_2 t_1 t_2 \rceil + 2.$$

Proof. First we prove that if G and H are two graphs such that $\delta(G) \geq 2$ and $\delta(H) \geq 2$, then $N(G \square H) \leq N(G) + N(H)$. To see this, One can check that if $\{A_1, A_2, \dots, A_{n_1}\}$ and $\{B_1, B_2, \dots, B_{n_2}\}$ are coverings of G and H respectively, then $\{A_1 \times V(H), A_2 \times V(H), \dots, A_{n_1} \times V(H)\} \cup \{V(G) \times B_1, V(G) \times B_2, \dots, V(G) \times B_{n_2}\}$ is a covering for the graph $G \square H$. So $N(C_{t_1} \square C_{t_2}) \leq 2\lceil \log_2 t_1 t_2 \rceil + 2$. Since $P_{t_1} \square P_{t_2}$ is a subgraph of $C_{t_1} \square C_{t_2}$, the result follows. \blacksquare

Theorem C. (Lovasz Local Lemma) *Suppose that A_1, \dots, A_l are events in a probability space with $\Pr[A_i] \leq p$ for all i . If each event is mutually independent of all the other events except for at most d of them, and if $ep(d+1) \leq 1$, then $\Pr[\bigcap_{i=1}^l \bar{A}_i] > 0$.*

In view of the Lovasz Local Lemma, we give an upper bound for $N(G, w; 1)$.

Theorem 6. *If G is a graph with t vertices, and m edges, then*

$$N(G, w; 1) \leq \left\lceil \frac{\log_2(e[D+1])}{-\log_2 q} \right\rceil ,$$

where

$$q = 1 - p^2(1-p)^w \quad , \quad 0 < p < 1$$

$$D = m \binom{t-2}{w} - (m - (w+2)\Delta) \binom{t-w-4}{w}$$

Proof. Let $A = [a_{ij}]$ be an $N \times t$ random matrix whose entries are mutually independent chosen from $\{0, 1\}$ such that $Pr(a_{ij} = 1) = p$, N to be determined. The columns of A are labelled by the vertices of G and assume that $V(G) = \{u_1, \dots, u_t\}$. Assign to the i^{th} row of A , the subset A_i of the vertices of G as follows

$$A_i = \{u_j | 1 \leq j \leq t, a_{ij} = 1\}.$$

For every edge $U = \{u_1, u_2\}$ and a subset W of vertices, where $W \subseteq V(G) \setminus U$ and $|W| = w$, let $A_{(U,W)}$ be the event that there does not exist a row of A such that all entries in the columns in U are 1 and all entries in the columns in W are 0. Note that $\mathcal{A} = \{A_1, A_2, \dots, A_N\}$ is a $(w; 1)$ -covering of G if and only if none of these events occur, that is, if $Pr(\cap \bar{A}_{(U,W)}) > 0$. One can check that

$$Pr(A_{(U,W)}) = q^N,$$

where

$$q = 1 - p^2(1-p)^w \quad \& \quad 0 < p < 1.$$

Note that the event $A_{(U,W)}$ is mutually independent of all the other events $A_{(U',W')}$ except those with

$$(U \cup W) \cap (U' \cup W') \neq \emptyset.$$

There are at most

$$D = m \binom{t-2}{w} - (m - (w+2)\Delta) \binom{t-w-4}{w}$$

such events. According to the Lovasz Local Lemma, a $(w; 1)$ -covering of G exists whenever

$$e(D+1)q^N \leq 1.$$

Taking logarithms of both sides of this inequality and rearranging, we get the desired result. ■

Acknowledgments: This paper is a part of Mehdi Azadi Motlagh's Ph.D. Thesis. The authors would like to express their deepest gratitude to Professor Hossein Hajiabolhassan to introduce a generalization of cover-free families and also for his invaluable comments and discussion.

References

- [1] Sergei Bezrukov, Dalibor Froněk, Steven J. Rosenberg, and Petr Kov. On biclique coverings. *Discrete Mathematics*, 308(23):319 – 323, 2008. [8](#)
- [2] Béla Bollobás and Alex Scott. Separating systems and oriented graphs of diameter two. *J. Combin. Theory Ser. B*, 97(2):193–203, 2007. [2](#)
- [3] A. G. Dyachkov and V. V. Rykov. Bounds on the length of disjunctive codes. *Problemy Peredachi Informatsii*, 18(3):7–13, 1982. [6](#)
- [4] P. Erdős, P. Frankl, and Z. Füredi. Families of finite sets in which no set is covered by the union of two others. *J. Combin. Theory Ser. A*, 33(2):158–166, 1982. [1](#), [6](#)
- [5] Zoltán Füredi. On r -cover-free families. *J. Combin. Theory Ser. A*, 73(1):172–173, 1996. [1](#), [6](#)
- [6] Hossein Hajiabolhassan and Farokhlagha Moazami. Secure frameproof codes through biclique covers. *Discrete Math. Theor. Comput. Sci.*, 14(2):261–270, 2012. [1](#), [3](#)
- [7] Hossein Hajiabolhassan and Farokhlagha Moazami. Some new bounds for cover-free families through biclique covers. *Discrete Mathematics*, 312(24):3626 – 3635, 2012. [1](#), [3](#)
- [8] G. Katona and E. Szemerédi. On a problem of graph theory. *Studia Sci.Math. Hungar.*, pages 23–28, 1967. [7](#)
- [9] W. Kautz and R. Singleton. Nonrandom binary superimposed codes. *Information Theory, IEEE Transactions on*, 10(4):363–377, Oct 1964. [1](#)
- [10] Hyun Kwang Kim and Vladimir Lebedev. On optimal superimposed codes. *Journal of Combinatorial Designs*, 12(2):79–91, 2004. [1](#)
- [11] Hyun Kwang Kim, Vladimir Lebedev, and Dong Yeol Oh. Some new results on superimposed codes. *J. Combin. Des.*, 13(4):276–285, 2005. [3](#)
- [12] Sh. Kh. Kim and V. S. Lebedev. On the optimality of trivial (w, r) -cover-free codes. *Problemy Peredachi Informatsii*, 40(3):13–20, 2004. [3](#)
- [13] P. C. Li, G. H. J. van Rees, and R. Wei. Constructions of 2-cover-free families and related separating hash families. *J. Combin. Des.*, 14(6):423–440, 2006. [3](#), [5](#)
- [14] Miklós Ruszinkó. On the upper bound of the size of the r -cover-free families. *J. Combin. Theory Ser. A*, 66(2):302–310, 1994. [1](#), [6](#)
- [15] D. R. Stinson, Tran van Trung, and R. Wei. Secure frameproof codes, key distribution patterns, group testing algorithms and related structures. *J. Statist. Plann. Inference*, 86(2):595–617, 2000. Special issue in honor of Professor Ralph Stanton. [3](#)

- [16] Douglas R Stinson and Ruizhong Wei. Combinatorial properties and constructions of traceability schemes and frameproof codes. *SIAM Journal on Discrete Mathematics*, 11(1):41–53, 1998. [3](#)
- [17] D.R. Stinson and R. Wei. Generalized cover-free families. *Discrete Mathematics*, 279(13):463 – 477, 2004. [1](#)
- [18] R. Wei. On cover-free families. *manuscript.*, 2006. [1](#)